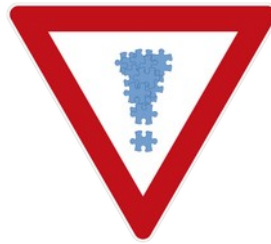


Enjoy IT Secured

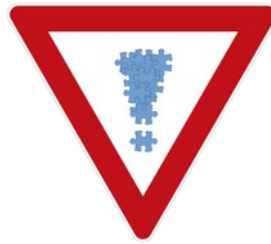


Einige Regeln, um Ihr System zu schützen

Sicheres und umsichtiges Verhalten ist neben der Verwendung der Virenschutz-software der beste Schutz vor schädlicher Software.

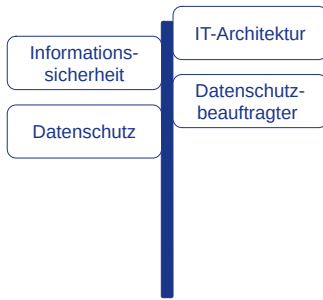
So verringern Sie Ihr Risiko und helfen Ihr System zu schützen:

1. Öffnen Sie keine E-Mail-Anhänge von unbekanntem, verdächtigen oder nicht vertrauenswürdigen Seiten. Öffnen Sie keinen E-Mail-Anhang, wenn die Betreffzeile fragwürdig ist.
2. Dies gilt auch dann, wenn Sie von einem bekannten Empfänger unerwartet große E-Mails bekommen. Öffnen Sie keinen Anhang einer E-Mail, wenn Sie nicht sicher sind, was es ist. Einige Schädlinge verbreiten sich per E-Mail und verwenden die E-Mail-Adresse eines bereits befallenen Systems.
3. Sichern Sie E-Mail-Anhänge bevor Sie sie öffnen. Dann kann der Virens Scanner die Datei sicher untersuchen.
4. Löschen Sie Kettenmails oder SPAM aus Ihrer Mailbox und leiten Sie sie nicht weiter.
5. Verwenden Sie keine HTML-formatierten E-Mails, schalten Sie entsprechende Optionen in Ihrem E-Mail-Programm aus. Hierin können sich Script-Viren verbergen.
6. Gehen Sie möglichst nicht ins Internet, wenn Sie als Benutzer mit Administrator-Rechten angemeldet sind.
7. Seien Sie vorsichtig, wenn Sie Dateien aus dem Internet laden. Vergewissern Sie sich, dass die Site vertrauenswürdig ist. Im Zweifelsfall verzichten Sie lieber auf den Download. Seien Sie besonders vorsichtig, wenn Sie Software aus dem Internet laden. Dies gilt besonders bei freier Software, die oft Adware oder anderen ungewollten Inhalt beinhaltet. Dies gilt auch für Screensaver, Spiele, Browser add-ons, peer-to-peer (P2P) Clients, besonders aber für "gecrackte" oder freie Versionen von ansonsten teuren Applikationen.
8. Dies gilt auch und insbesondere für Dateien, die Sie aus einer Newsgroup, dem IRC oder per WWW- oder FTP-Download erhalten haben. Links aus IRC und In-

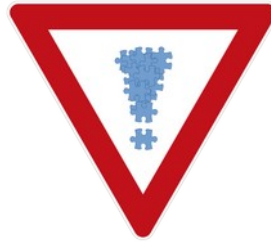


stant Messaging verweisen im hohen Umfang auf infizierte Downloads.

9. Auch Original-CD-ROMs und -Disketten können Viren enthalten. Prüfen Sie daher auch diese vor der Benutzung ebenso sorgfältig wie andere Datenträger. CD-ROMs aus Zeitschriften und solche, die als kostenlose Werbemittel verteilt werden, werden meist weniger sorgfältig geprüft, bevor sie in Umlauf gebracht werden.
10. Entfernen Sie den Schreibschutz Ihrer externen Speichermedien (Disketten, USB-Sticks) nur dann, wenn Sie Dateien darauf schreiben wollen. Schreibgeschützte Medien können nicht infiziert werden.
11. Öffnen Sie keine Dateien von externen Medien, ohne sie mit einem Antivirus-Programm geprüft zu haben. Dies gilt insbesondere – aber nicht nur - für Dokumente von MS Word und alle anderen MS-Office-Anwendungen.
12. Fertigen Sie regelmäßig, mindestens wöchentlich, Sicherheitskopien Ihrer wichtigen Daten an. Bei der Reparatur einer infizierten Datei durch das Virenschutzprogramm könnte diese beschädigt oder sogar unbrauchbar werden.
13. Wachsamkeit ist der beste Schutz gegen Phishing-Angriffe. Wenn Sie E-Mails erhalten, in denen Sie aufgefordert werden, Kontoinformationen zu aktualisieren, so antworten Sie nicht auf diese E-Mails und klicken Sie auf keinen Fall auf einen eventuell enthaltenen Link.
14. Geben Sie Internetadressen direkt im Browser ein oder rufen sie aus einem Lesezeichen aus auf. Zugesandte Links können zu gefälschten Seiten führen, die teilweise täuschend echt aussehen.
15. Überprüfen Sie ihre Online-Konten regelmäßig. Durch einen Identitätsdiebstahl könnten sich Kriminelle Zugang zu Ihren Onlinekonten verschaffen und von dort Überweisungen veranlassen. Aber auch Ihre Internetzugänge bei eBay oder Amazon.de, um nur Beispiele zu nennen, können zu Ihrem Nachteil missbraucht werden.
16. Aktualisieren Sie ihre Virenschutzsoftware regelmäßig. Bedrohungen wachsen beständig und entwickeln sich ständig weiter. Hunderte von neuen Viren werden monatlich entdeckt. Um sicherzustellen, dass sie gegen diese Bedrohungen geschützt sind, aktualisieren Sie Ihre Virenschutzsoftware und die Viren Signatur-Dateien regelmäßig.



Enjoy IT Secured



17. Aktualisieren Sie Ihr Betriebssystem und Ihre Anwendungen, wie Internet-Browser, E-Mail-Clients, aber auch Multimedia-Anwendungen, wenn neue Sicherheits-Patches vorliegen.
18. Verwenden Sie eine Personal Firewall.
19. Lassen Sie sich im Windows-Explorer die Dateierweiterungen anzeigen (Im Explorer mit Tools-Menü: Tools/Folder Options/View – entfernen Sie dort das Häkchen bei "Hide file extensions for known file types"). Damit wird es erschwert, eine gefährliche Datei (wie z.B. EXE) hinter einem harmlos klingenden Dateinamen (wie z.B. TXT oder JPG) zu verbergen.
20. Öffnen Sie niemals E-Mail-Anhänge mit Dateitypen VBS, SHS oder PIF. Die Arten von Dateianhängen werden so gut wie nie versendet, sind aber häufig Träger von schädlicher Software.
21. Öffnen Sie niemals Anhänge mit doppelter Dateierweiterung wie z.B. NAME.BMP.EXE oder NAME.TXT.VBS.
22. Stellen Sie ihr E-Mail-Programm so ein, dass Anhänge nicht automatisch geöffnet werden und verzichten Sie möglichst auf die Auto-Vorschau (insbesondere bei Outlook Express).